Lurie Besikof Lapidus & Company, LLP

MAXIMUS
California Healthy Families Project

Information Security

March 1, 2009 to July 31, 2009

Table of Contents

Section Page

SECTION ONE

Internal Auditor’s Report

Lurie Besikof Lapidus & Company, LLP

SECTION ONE – INTERNAL AUDITOR'S REPORT

Report by Lurie Besikof Lapidus & Company, LLP

Mr. Bruce Caswell, President, MAXIMUS Operations Group
Reston, Virginia

We have performed tests of management's assertions (Section Four) about the internal control structure with respect to the information security maintained by the MAXIMUS California Healthy Families Project (the Project) during the period of March 1, 2009 to July 31, 2009, and its compliance under contract 02MHF026 (Contract) with the State of California Managed Risk Medical Insurance Board (MRMIB) (Specified Requirements) related to the California Healthy Families program. We have also performed various tests of information security compliance with appropriate Business Rules, Process Procedures and Work Instructions. The Project's Business Rules, Process Procedures and Work Instructions are meant to assure compliance by the Project with the Contract requirements. Management of the Project is responsible for the Project's compliance with the Contract requirements. The sufficiency of the tests is solely the responsibility of Management. Consequently, we make no representation regarding the sufficiency of the procedures for the purpose for which this report has been requested or for any other purpose.

Because of inherent limitations in any internal control structure, misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control structure to future periods are subject to the risk that the internal control structure may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Any exceptions to management's assertions with respect to the information security control structure by the Project during the period March 1, 2009 to July 31, 2009, and compliance with the Project's Business Rules, Process Procedures and Work Instructions over information security are presented in Section Four – Results.

This report is intended solely for the information and use of MAXIMUS Operations Group, the MRMIB, and the auditors of the State of California and is not intended to be and should not be used by anyone other than those specified parties.

Lurie Besikof Lapidus & Company, LLP

Lurie Besikof Lapidus & Company, LLP
March 15, 2010

612.381.8939
612.377.1325

2501 Wayzata Boulevard
Minneapolis, MN 55405-2197

www.lblco.com

SECTION TWO

Executive Summary

SECTION TWO – EXECUTIVE SUMMARY

Overview

This report summarizes the results of our internal audit procedures related to the internal control structure with respect to the information security maintained by the MAXIMUS California Healthy Families Project (the Project) during the period March 1, 2009 to July 31, 2009, and its compliance under contract 02MHF026 (Contract) with the State of California Managed Risk Medical Insurance Board (MRMIB) related to the California Healthy Families program (the Program). This report also covers tests performed relating to compliance with the Project's Business Rules, Process Procedures and Work Instructions over information security.

This report covers the results of the internal audit covering information security maintained by the Project along with any recommendations to improve the controls of information security.

Assertions, Tests and Results

Our procedures were designed to test the information security maintained by the Project and its compliance under the Contract with the MRMIB related to the Program during the period.

In all cases where sampling was performed, a random selection algorithm was utilized. The sample quantity selected assumed either a finite population where possible or an infinite population with a 95% confidence level, a 5% expected error rate in the population, and a 5% error rate in sampling and testing.

The following are the assertions tested based on the contract provisions:

Logical Security:

- Project Information Technology (IT) operating systems and subsystems are secured to prevent unauthorized use, disclosure, modification, damage or loss of data. The key objectives of Logical Security include:
  - Appropriate authentication of system users
  - Regular password change requirements
  - Timely action relating to requesting, establishing, issuing, suspending and closing user accounts
  - Appropriate use of firewalls, intrusion detection and vulnerability assessments
  - Maintenance of logs for security activities, and security violations and the monitoring for the appropriate reporting to senior management
  - Physical security related to facility access relating to only authorized personnel and a requirement for appropriate identification and authentication
  - The use of only authorized software on project IT assets
  - The proper configuration of application software and data storage systems providing access based on the individual's demonstrated need to view, add, change or delete data
  - The use of virus protection

Data Backup and Off-Site Storage:

- Backup process for critical and sensitive data is occurring as described and adequate to provide for emergency recovery if needed. The key objectives data backup and off-site storage are:
  - Periodic off-site inventories are performed to assure that backups are accessible and secure
  - Complete daily backups are created when the database is not in an update mode (after hours) on a daily basis
  - Backups of data files are rotated off-site on a regular and secure manner

Change Control and Data Integrity:

- Change control processes are in operation and implemented. The key objectives of change control and data integrity are:
  - Application and system modifications are aligned with the client (the MRMIB) and/or MAXIMUS specifications
  - Users are appropriately involved in the design of applications, selection of packaged software and their testing to ensure a reliable environment
  - Information systems are designed to include application controls that support complete, accurate, authorized, and valid transaction processing
  - Post-implementation reviews are performed to verify controls are operating effectively
  - Changes are properly tested prior to implementation
  - Proper segregation of duties exists between developers, testers, and users
  - The testing and development environment are segregated from the production environment
  - Source code is segregated and maintained off the production environment
  - Approvals are received prior to migration of code to the production environment
  - Conversion of data is tested between its origin and its destination to confirm that it is complete, accurate and valid
  - Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid

Physical Security:

- Access to the facility is granted by a badging system that is maintained to contain access for active employees only.
- Access to the data center is restricted to authorized personnel, requiring appropriate identification and authentication.
- Data center facilities are equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), and air conditioning.

Sampling Method

Where sampling was performed, a random selection algorithm was utilized. The sample quantity selected used a population size that was provided with a 95% confidence level, a 5% expected error rate in the population, and a 5% error rate in sampling and testing.

Detailed results along with the tests performed are presented in Section Four – Results of this report.

Exceptions Noted

Logical Security

1. User passwords are changed regularly; however two (2) user accounts out of six-hundred-thirty-seven (637) active enabled user accounts (.31%) are unable to change their passwords every ninety (90) days since they do not login directly in to the domain. Additionally, noted that these two (2) user accounts are flagged to never expire.

   MAXIMUS Response

   The two user accounts unable to change their passwords every ninety days are Corporate user accounts. Because Corporate user accounts access network resources with an automated login behind the scenes, they do not receive warning messages regarding password expiration and cannot change their passwords.

   If their passwords were set to expire, it would happen with no warning and they would suffer a work stoppage until access was restored. This is a known solution that was designed and implemented to balance security and business effectiveness. To be consistent with the current password change policy, the passwords for the Corporate user accounts will be manually reset every 90 days.

   Problem Statement #62457 has been created to document the manual reset of Corporate accounts and to develop a monitoring process to ensure compliance.

External Vulnerability Testing

1. Relevant warnings were discovered. Warnings are medium risk vulnerabilities that could potentially permit damage and should be resolved as soon as possible. Note that these findings are of a lesser nature than true holes. This is since warning level vulnerabilities require more advanced knowledge to exploit than hole level vulnerabilities.

   MAXIMUS Response:

   Problem Statement #62458 has been created to document this element and track resolution.

Internal Vulnerability

1. Internal vulnerability testing disclosed some warnings and holes. These warnings and holes are delineated between two segments as follows:
   a. Privileged Segment

   b. User Segment

   MAXIMUS Response:

   The Privileged Segment of the network provides access to servers by IS personnel who maintain systems and certain professional "Power User" staff in the normal course of their duties.

   The User Segment of the network is accessed by Business Unit personnel via the software used in the normal course of their duties (eligibility and enrollment system, Oracle Financials, etc.).

   We are currently engaged in a technology refresh, including a network redesign and software and hardware upgrades. This effort incorporates best practices for network segregation and the elements identified will be eliminated.

   Problem Statement #62459 has been created to document these elements and track resolution.

Physical Security – Badge Holders

1. One (1) of five-hundred-seventy (570) badge holders (.175%) was no longer employed by the Project. However, this threat is mitigated by the fact that badges are disabled after five (5) days of non-use. In four (4) additional cases, badges were misclassified where a vendor was given employee classification badge access. Note that this issue is mitigated by the fact that the employee classification is as an Administrative Assistant. An Administrative Assistant has a lesser set of access privileges than a vendor classification.

   MAXIMUS Response:

   One (1) exception of five (5) instances occurred due to a misclassification of role assignment.

   A former employee, terminated in 2006, was found in the security database because she was misclassified as a vendor. The ID badge and role assignment for four (4) external auditors was done without clarity of what designation should be provided. The designation of Administrative Assistant was the most common and lowest risk of all designations as it provides minimal access with the access card deactivating after five (5) days of inactive usage.

   As a continual improvement initiative, Problem Statement # 62461 was created to further enhance the current Policy and Procedure documents for the ID and role assignment. Furthermore, the effectiveness of weekly monitoring of terminations against the security database will be evaluated to ensure accuracy.

Recommendations

In addition to the exceptions noted above, we also offer the following suggestion to further strengthen the information security controls in the Project.

1. While data on backup tapes is encrypted and can only be read by servers located in the data center, we found that several tapes were located in an unsecured desktop drawer at risk for potential misuse by unauthorized personnel and possible moisture or dust damage, potentially restricting further use of tapes. Our recommendation would be to store all backup tapes in a secure, locked location, where only authorized personnel will be able to access them. Furthermore, they should be located in an area protected from moisture or dust damage that could jeopardize the future use of the backup tapes.

   MAXIMUS Response:

   The tapes described in the finding were being used to rebuild a file server, and were logged out and tracked appropriately. At night the tapes were stored in a locked drawer in the work area of the System Administrator using them.

   In the future, in consideration of the environmental factors described, all tapes will be stored in the data center when not in direct use.

   Problem Statement #62460 has been created to enhance the current procedures for tape storage while checked out for use.

SECTION THREE

Scope and Objectives

SECTION THREE – SCOPE AND OBJECTIVES

Scope of the Internal Audit

The scope of this internal audit engagement was to examine the Project's information systems controls designed to meet the provisions of the Project's Contract with the MRMIB. The scope of the examination related to the period from March 1, 2009 to July 31, 2009, related to the protection of the Project's data and information contained on the systems administered by MAXIMUS.

Objective of the Internal Audit

The overall objective of this internal audit engagement was to verify the Project's controls and procedures ensure that the information in the custody of MAXIMUS is secure, has integrity and is available.

SECTION FOUR

Results

SECTION FOUR – RESULTS

The components, testing procedures performed and results are listed below.

Component Tested	Testing Procedure Performed	Results
1. Logical Security		
1.1 Documentation exists for Project IT operating systems and subsystems assuring that all systems are secured to prevent unauthorized use, disclosure, modification, damage or loss of data.	• *Obtained and inspected* copies of the: ▪ security policy; ▪ security strategy or strategies; ▪ security procedures and standards; ▪ network inventory or schematic of physical network components; ▪ network problem tracking, resolution and escalation procedures; ▪ security violation reports and management inspection procedures; ▪ lists of vendors and customers with access to the network; and ▪ relevant legal and regulatory information related to security and information access.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* a statistically valid sample of employee personnel files verifying the presence of signed user security awareness documents.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* a statistically valid sample of employee personnel files verifying the existence of new employee training materials relating to security.	No exceptions noted. The documentation inspected confirms management's description.

Component Tested	Testing Procedure Performed	Results
1.2 Data owners have been identified for all information assets. A value has been assigned to each information asset (high, medium, low) that represents the cost to the organization should the asset be compromised.	• *Obtained and inspected* a list of information assets verifying that each asset has an assigned owner and relative value.	No exceptions noted. The documentation inspected confirms management's description.
1.3 The Project maintains a network inventory and/or topology diagram that identifies all physical access points to the information assets.	• *Obtained and inspected* current network topology diagram. • *Inquired* of appropriate network personnel regarding all physical access points to the information assets and their identification.	No exceptions noted. The documentation inspected confirms management's description. No exceptions noted. Inquiries confirm management's description.
1.4 The Project maintains documentation identifying and classifying all connections to the network based on the level of control required by the security policy. The four potential classifications for interconnected systems are: ▪ Trusted—Represents systems that are under direct control of the organization ▪ Semi-trusted—Requires authenticated access to protect exposed systems not accessible by the public ▪ Un-trusted—Requires authenticated access to specific information resources on exposed publicly accessible systems ▪ Hostile—Very restricted access only	• *Inquired* of appropriate IT management regarding classification of each network connection. • *Inquired* of appropriate IT network personnel to determine if all physical access points to the information assets have been identified.	No relevant exceptions noted. The Project appropriately classifies each DMZ segment based on risk. Inquiries confirm the essence of management's description. No exceptions noted. Inquiries confirm management's description.

Component Tested	Testing Procedure Performed	Results
	• *Obtained and inspected* the firewall and the router configurations to evaluate the Demilitarized Zone (DMZ) architecture and verify the appropriate trust classifications and protocols associated with the connections to the network services[1].	No exceptions noted. The documentation inspected confirms management's description.
	• *Inspected* the firewall and the router configuration documentation verifying that the trusted network is segmented from the semi-trusted, un-trusted and hostile network. Verified that the trusted network is on a separate segment where services such as e-mail, web, FTP, etc. access from outside connections are classified into appropriate trust zones and partitioned or segmented appropriately.	No exceptions noted. The documentation inspected confirms management's description.

[1] Network services are hardware and/or software installed and operating on network servers that advertise and provide the foundation computing environment. Network services provide actions as necessary to ensure the integrity of the distribution network and maintain the capability of providing file transfer, email, web services, and other items.

Component Tested	Testing Procedure Performed	Results
1.5 The Project maintains access roles and category schemes to determine if the access privileges granted users are restrictive enough to limit risks from malicious users. The Project employs the concept of least privilege[2].	• *Obtained and tested* a listing of: ▪ employees terminated during the period under examination; ▪ current employees including their role within the organization; ▪ temporary employees including start and end dates; and ▪ access rights and roles for the system and Oracle Financials. By verifying: ▪ access rights have been removed for all terminated employees; ▪ user passwords are changed regularly; and ▪ appropriate roles are assigned to employees based on need in the system and Oracle Financials.	Verification indicated that: • access rights have been removed for all terminated employees, and • appropriate roles are assigned to employees based on need in the system and Oracle Financials. However, noted that two (2) user accounts out of six-hundred-thirty-seven (637) active enabled user accounts (.31%) are unable to change their passwords every ninety (90) days since they do not login directly in to the domain. Additionally, noted that these two (2) user accounts are flagged to never expire. MAXIMUS Response: The two user accounts unable to change their passwords every ninety days are Corporate user accounts. Because Corporate user accounts access network resources with an automated login behind the scenes, they do not receive warning messages regarding password expiration and cannot change their passwords. If their passwords were set to expire, it would happen with no warning and they would suffer a work stoppage until access was restored. This is a known solution that was designed and implemented to balance security and business effectiveness. To be consistent with the current password change policy, the passwords for the

[2] The concept of least privileges provides that each subject is granted only the necessary rights to complete their assigned job duties.

Component Tested	Testing Procedure Performed	Results
		Corporate user accounts will be manually reset every 90 days. Problem Statement #62457 has been created to document the manual reset of Corporate accounts and to develop a monitoring process to ensure compliance.
	• *Inquired* of the department managers to identify the appropriate employee roles assigned in the respective department.	No exceptions noted. Inquiries confirm management's description.
	• *Inspected* the access role and category schemes to determine if the access privileges granted users are restrictive enough to limit risks from malicious users.	No exceptions noted. The documentation inspected confirms management's description.
1.6 The Project maintains a network topology[3] which segments differing trust levels, and limits external services and protocols to only those which are necessary to conduct the business and maintenance of the organization.	• *Obtained and inspected* current network diagrams/schematics to verify that routers and switches are installed between network segments of differing trust levels.	No exceptions noted. The documentation inspected confirms management's description.
	• *Inquired* of the network administrator regarding services and protocols enabled on external routers/firewalls.	No exceptions noted. Inquiries confirm management's description.
	• *Obtained and inspected* the router and firewall configurations to verify that all unnecessary services and protocols have been disabled.	No exceptions noted. The documentation inspected confirms management's description.

[3] The network topology is the pattern of interconnections between the network components in the computing environment.

Component Tested	Testing Procedure Performed	Results
1.7 The Project maintains network infrastructure configurations which limit access via the network to only those who have a need to do so. Where network configurations are saved in a clear text format they are sanitized so as to not contain password related information.	• *Obtained and inspected* configuration files from external routers and firewalls. Verified that all encrypted passwords have been removed from the configuration files and that access points to routers have been limited to IP addresses used by authorized network administrators.	No exceptions noted. The documentation inspected confirms management's description.
	• *Inquired* of appropriate staff regarding the use of modems connected to router auxiliary ports. Verifying that sufficient control exits to limit access to only authorized individuals.	Noted that two (2) servers have modems used by external vendors. These modems are disabled until the vendor requests access, then immediately disabled after the vendors competes any necessary work. No exceptions noted. The inquiry confirms management's description.
	• *Obtained and inspected* the network diagrams for the placement and use of switches in the network topology.	No exceptions noted. The documentation inspected confirms management's description.
	• *Verified* through review of configuration documentation and inquiry of appropriate personnel that the network administrator has taken steps to limit access and protect passwords for devices which are configured for remote monitoring.	No exceptions noted. The documentation inspected and inquiries confirm management's description.

Component Tested	Testing Procedure Performed	Results
1.8 The Project utilizes external routers and firewalls in accordance with policies and best practices. This includes the use of: ▪ External routers for filtering invalid traffic to prevent spoofing attacks and limit unnecessary filtering processing by firewalls and other devices. ▪ Firewalls for granular filtering of traffic through the use of stateful and dynamic inspection.	• *Obtained and inspected* the configurations from external routers verifying that external routers are filtering traffic: ▪ with a source address that is internal to the network; ▪ within the range of invalid or private addresses; ▪ with the loopback address of 127.0.0.1; ▪ with IP options set such as source routing; ▪ traffic destined for the broadcast address of a subnet; ▪ incoming ICMP[4] traffic; and ▪ all outgoing traffic except that with a source address internal to the network. In addition, verified that external routers are not performing granular filtering functions.	No exceptions noted. The documentation inspected confirms management's description.
	• *Inquired* of application, system and network administrators as to the completeness and documented understanding of what must be permitted into and out of the Project's network.	No exceptions noted. Inquiries confirm management's description.

[4] ICMP or Internet Control Message Protocol is a protocol used to send error and control messages.

Component Tested	Testing Procedure Performed	Results
1.9 Appropriate firewall devices have been implemented which: ▪ support the business needs of the Project; ▪ deny all traffic unless explicitly allowed; and ▪ prevent VPN[5] terminations to un-trusted networks as encrypted VPN traffic precludes any inspection process by a firewall.	• *Inquired* of the network administrator the reasoning behind the architecture and type of firewall installed. • *Obtained and inspected* the firewall configuration and rule set to verify that : ▪ all traffic is denied unless explicitly permitted; and ▪ the firewall default implicit rule set usually shipped with a firewall to is not circumventing the implicit firewall rules. • *Obtained and inspect* documentation regarding the termination of VPNs to assure that termination is possible only to trusted networks.	No exceptions noted. Inquiries confirm management's description. No exceptions noted. The documentation inspected confirms management's description. No exceptions noted. The documentation inspected confirms management's description.

[5] VPN or Virtual Private Network is a private network that is configured within the Internet in order to take advantage of the economies of scale and management facilities of large networks.

Component Tested	Testing Procedure Performed	Results
1.10 By appropriately configuring network devices, applications and services, the Project maintains a secure network. In addition the Project identifies potential vulnerabilities by periodically conducting network security assessments.	• *Obtained* external and internal IP addresses to be tested. • *Performed* external network vulnerability testing.	No exceptions noted. External and internal IP addresses were obtained as requested. The external vulnerability assessment indicated relevant warnings. Warnings are medium risk vulnerabilities that could potentially permit damage and should be resolved as soon as possible. Note that these findings are of a lesser nature than true holes. This is since warning level vulnerabilities require more advanced knowledge to exploit than hole level vulnerabilities. The list of vulnerabilities found is being delivered under separate cover to MAXIMUS for resolution as these vulnerabilities are typically considered sensitive in nature. MAXIMUS Response:

Component Tested	Testing Procedure Performed	Results
		Problem Statement #62458 has been created to document this element and track resolution.

Component Tested	Testing Procedure Performed	Results
	• *Performed* an internal network vulnerability test as both a privileged network segment and a user network segment.	Privileged Segment User Segment MAXIMUS Response: The Privileged Segment of the network provides access to servers by IS personnel who maintain systems and certain professional "Power User" staff in the normal course of their duties. The User Segment of the network is accessed by Business Unit personnel via the software used in the normal course of their duties (the system, Oracle Financials, etc.). We are currently engaged in a technology refresh, including a network redesign and software and hardware upgrades. This effort incorporates best practices for network segregation and the elements identified will be eliminated. Problem Statement #62459 has been created to document these elements and track resolution.

Component Tested	Testing Procedure Performed	Results
	• *Inquired* of IT management if periodic vulnerability testing is an integral function of information security.	Per discussions with IT management, periodic testing is performed; however, the process is not formalized. MAXIMUS Corporate is in the process of developing a formalized process. No relevant exceptions noted. Inquiries confirm management's description.
	• *Inquired* of IT management if goals and objectives of vulnerability testing been documented and approved.	No exceptions noted. Inquiries confirm management's description.
	• *Inquired* of IT management if the results of tests are properly documented and shared with the appropriate people who can respond to any identified weaknesses.	No exceptions noted. Inquiries confirm management's description.
1.11 The Project utilizes anti-virus software to protect its information assets.	• *Inquired* of IT management regarding the use of anti-virus software.	No exceptions noted. Inquiries confirm management's description.
	• *Obtained and inspected* the security policy noting the use of virus protection on information assets.	No exceptions noted. The documentation inspected confirms management's description.
	• *Inspected* a sample of employee workstations for the use of anti-virus software.	No exceptions noted. Inspected fifteen (15) workstations. The inspections confirm management's description.

Component Tested	Testing Procedure Performed	Results
2. Data Backup and Off-Site Storage		
2.1 The Project has established backup and recovery policies and procedures to assure that critical data are available.	• *Obtained and inspected* the backup procedures followed for each system.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* the backup logs noting any errors or warnings.	No exceptions noted. The documentation inspected confirms management's description.
	• *Observed* if the backup and recovery procedures are being followed.	No exceptions noted. The observations confirm management's description.
	• *Observed* a test restore documenting the results of the test restore performed.	No exceptions noted. The observations confirm management's description.

Component Tested	Testing Procedure Performed	Results
2.2 The Project utilizes an off-site storage facility to assure that backed-up data is protected in the event of a disaster at the primary data processing facility.	• *Inspected* the off-site storage facility validating the facility is adequate based upon the location: ▪ being a sufficient distance from the Project offices; ▪ possessing access roads with alternate routing; ▪ providing accessibility within a reasonable period of time; ▪ an adequate distance from high-risk areas; ▪ in rural and low-traffic area; ▪ has an absence of glass windows; ▪ has a security system; ▪ has a limited number of access doors; ▪ has a mantrap area; ▪ has enforced sign-in logs; ▪ has visitor badges and escort practices; ▪ has unmarked bin storage; ▪ has bonded employees; ▪ is not located in the same area as high-risk facilities; ▪ has several levels of fire detection and suppression; ▪ has temperature and humidity monitoring; ▪ has telephone and electrical underground lines; and ▪ has and internal loading dock.	No exceptions noted. The inspection confirms management's description.

Component Tested	Testing Procedure Performed	Results
2.3 The Project employs rotation practices at the off-site storage facility to assure that backed-up data is protected in the event of a disaster at the primary data processing facility.	• *Obtained and inspected* the log of tapes stored at the off-site storage facility. • *Tested* the log of tapes stored at the facility by physically comparing it with the items present at the facility. • *Inquired* of IS personnel to determine how often the log is inspected for completeness and accuracy.	No exceptions noted. The documentation inspected confirms management's description. No exceptions noted. The testing of log tapes confirms management's description. No exceptions noted. Inquiries confirm management's description.
2.4 The Project ensures that appropriate cross-training on all backup and restore procedures occurs.	• *Inquired* of IS personnel to determine if cross-training is performed for backup, restore and requesting tapes from the off-site storage. • *Inspected* available training records to determine the amount of cross-training provided on backup and restore procedures	No exceptions noted. Inquiries confirm management's description. No exceptions noted. The documentation inspected confirms management's description.

Component Tested	Testing Procedure Performed	Results
3. Change Control and Data Integrity		
3.1 The Project has implemented proper change control processes.	• *Obtained and inspected* documentation detailing the processes and procedures in place to determine: ▪ who prioritizes and justifies changes; ▪ how user requests are assigned to programmers; ▪ how testing is performed; ▪ who approves changes; and ▪ how edited or new programs are put into production, etc.	No exceptions noted. The documentation inspected confirms management's description.
	• *Verified* that adequate guidelines are established to instruct programming personnel in their duties.	No exceptions noted. The documentation inspected confirms management's description.
3.2 The Project tracks and acts upon change requests for the production environment.	• *Inquired* of appropriate management to verify all requests for system amendments are considered for action and that all approved requests are implemented on a timely basis.	No exceptions noted. Inquiries confirm management's description.
	• *Obtained and inspected* a sample of CARs documentation identifying that adequate procedures were in place to ensure that systems, operations, and clerical documentation are properly updated.	Eleven (11) CARs were selected for inspection out of the forty-six (46) CARs initiated during the period March 1, 2009 to July 31, 2009. No exceptions noted. Documentation inspected confirms management's description.

Component Tested	Testing Procedure Performed	Results
	• *Verified* there is adequate involvement from all areas along with appropriate approval of system modifications by: ▪ application owners; ▪ users; ▪ relevant IT personnel; ▪ security personnel; and ▪ the MRMIB.	No exceptions noted. The information verified confirms management's description.
	• *Verified* appropriate segregation of duties related to: ▪ developers/programmers examination rights; ▪ developers/programmers change rights; and ▪ promotion of changes to production.	No exceptions noted. The information verified confirms management's description.
	• *Obtained and inspected* the procedures for emergency changes.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* the procedures for out-of-hours emergencies, i.e. controls may include one-time emergency password, retained by the shift manager.	No exceptions noted. The documentation inspected confirms management's description.
	• *Inquired* of appropriate management as to the procedures in place for one-time changes (i.e., correction of a record, etc.)	No exceptions noted. Inquiries confirm management's description.

Component Tested	Testing Procedure Performed	Results
3.3 The Project has change control processes implemented for application test procedures.	• *Inquired* of appropriate management regarding the CAR testing procedures.	No exceptions noted. Inquiries confirm management's description.
	• *Verified* application testing procedures are performed by persons other than those involved in writing the programs.	No exceptions noted. The information verified confirms management's description.
	• *Verified* application testing procedures are performed by persons: ▪ sufficiently knowledgeable and trained in testing procedures; ▪ using a predetermined standard of testing; and ▪ documenting evidence of the testing and retaining the documented evidence.	No exceptions noted. The information verified confirms management's description.
	• *Verified* that adequate controls exist and are followed to prevent production files from being used during testing.	No exceptions noted. The information verified confirms management's description.
	• *Obtained and inspected* testing procedures for selected sample to ensure procedures are adequate to prevent any unauthorized coding from being inserted into programs prior to promotion into production.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* the test plan ensuring that there is a structured approach in use.	No exceptions noted. The documentation inspected confirms management's description.
	• *Verified* that the testing process involves regression testing checking of the individual modified/changed/new programs and of their effect on the entire system.	No exceptions noted. The information verified confirms management's description.

Component Tested	Testing Procedure Performed	Results
	• *Verified* that actual test results are documented and compared against expected results.	No exceptions noted. The information verified confirms management's description.
	• *Obtained and inspected* changes during the period under examination to ensure that discrepancies were highlighted for further investigation followed-up on.	No exceptions noted. The documentation inspected confirms management's description.
3.4 The Project has supervision and segregation of testing activities.	• *Verified* the appropriate level of supervision is in place.	No exceptions noted. The information verified confirms management's description.
	• *Obtained and inspected* user acceptance testing and determine if it is carried out in an appropriate environment, isolated from the production system.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* the procedures for the set up of test data.	No exceptions noted. The documentation inspected confirms management's description.
	• *Obtained and inspected* the procedures volume testing.	No exceptions noted. The documentation inspected confirms management's description.

Component Tested	Testing Procedure Performed	Results
4. Physical Security		
4.1 The Project has restricted access to the facility and data center, with limited badge access.	• *Inquired* of the appropriate IT management regarding the limited and restricted access to the facility and data center. • *Tested* the active badge database for the facility by comparing it against the active employee list to ensure only active employees have access.	No exceptions noted. Inquiries confirm management's description. One (1) of five-hundred-seventy (570) badge holders (.175%) was no longer employed by the Project. However, this threat is mitigated by the fact that badges are disabled after five (5) days of non-use. In four (4) additional cases, badges were misclassified where a vendor was given employee classification badge access. Note that this issue is mitigated by the fact that the employee classification is as an Administrative Assistant. An Administrative Assistant has a lesser set of access privileges than a vendor classification. MAXIMUS Response: One (1) exception of five (5) instances occurred due to a misclassification of role assignment. A former employee, terminated in 2006, was found in the security database because she was misclassified as a vendor. The ID badge and role assignment for four (4) external auditors was done without clarity of what designation should be provided. The designation of Administrative Assistant was the most common and lowest risk of all designations as it provides minimal access with the access card deactivating after five (5) days of inactive usage.

Component Tested	Testing Procedure Performed	Results
		As a continual improvement initiative, Problem Statement # 62461 was created to further enhance the current Policy and Procedure documents for the ID and role assignment. Furthermore, the effectiveness of weekly monitoring of terminations against the security database will be evaluated to ensure accuracy.
	• *Tested the* badge access to the data center with the security badge provided by the Project.	No exceptions noted. The tests performed confirm management's description.
4.2 The Project has adequate environmental controls within the data center.	• *Inquired* of the appropriate IT management regarding the environmental controls in place in the data center.	No exceptions noted. Inquiries confirm management's description.
	• *Obtained and inspected* the environmental controls in place in the data center identifying adequate air, power, etc.	Noted cardboard boxes and storage of hardware within the data center; however, they are in the process of performing several upgrades. No exceptions noted. The controls inspected confirm management's description.